St. Michael's College School	Technology, Privacy and Intellectual Property
Policy: Responsible Use of Technology and Social Media	**F1.07.20**

A. PURPOSE:

In light of our vision to educate young men for lives of faith, character and service, it is important that we prepare our students for success in life and work by providing them with electronic access to a wide range of information, as well as opportunities to develop relevant skills and to actively participate in the global community. St. Michael's College School (the "**School**") recognizes the impact of information technology on society. We have a responsibility to ensure that all learners develop a respect for the power of information technology and that technology is used ethically to promote values consistent with Catholic teachings and the Catholic Graduate Expectations.

This Responsible Use of Technology Policy (the "**Policy**") is in effect as of September 2020. Throughout the course of the 2020-2021 academic year, the School will gradually leverage more technology in our classroom pedagogy. Beginning in September 2021, the School will implement a Bring Your Own Device ("**BYOD**") program. The intent of this program is to further embrace the use of digital technology, foster responsible digital citizenship, support inquiry-based learning environments and enhance digital literacy, creativity, innovation, critical thinking and collaboration.

The use of information technology is a support for staff to perform their daily operational activities and work. Information technology provides staff further opportunities for professional development and relationship building in service to the School community and public.

The School's use of an electronic communication system has an educational and professional purpose, encompasses professional and career development and administrative services that support education.

The utilization of technology by all Users (as defined below) must uphold an equitable culture of caring, inclusion, dialogue, and learning and should always strive to respect the dignity of the human person.

B. DEFINITIONS

Copyright: the protection of creative works and authors' rights.

Cyberbullying: the use of information and communication technologies by an individual or group that is intended to harm others.

Electronic Communication: includes but is not limited to internet use, e-mail, social media, browsing, publishing or posting on web sites, downloading, accessing or storing files, and use of Personal Electronic Devices.

Intellectual Property (IP): property created using original thought such as art, inventions, creative writing, designs, software code, musical works, business plans, websites and technology, etc.

Internet: refers to an electronic communication system connecting thousands of computers all over the world through which millions of individual subscribers can interact and share information.

Internet Content Filtering: technology commonly used by schools to prevent users from viewing inappropriate web sites or content.

Personal Electronic Devices (PEDs): personally owned portable electronic handheld equipment and technology devices, which can be used for the purpose of communication, entertainment, data management, word processing, wireless internet access, image capture/recording, sound recording and information transmitting and/or receiving, including but not limited to cell phones, smart phones, smart watches, pagers, still/video cameras, computers, tablets and recording devices.

Plagiarism: taking the ideas, writings, or images of others and presenting them as if they were original to the user.

School Network: all School-owned or controlled (or used by the School under license for the School's purpose and activities) database / records systems, networks, cabling, and School-associated cloud services, School email, voicemail, fax transmissions, and including the use of and access to the School intranet and the internet.

School Technology: any technology which is owned or controlled by the School, or used by the School under licence, for the School's purpose and activities, including all computers and mobile or portable devices, hardware, and software using School Technology.

Social Media: a form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content.

Spam E-mail (or shortened to "Spam"): the common term for unsolicited e-mail.

Users: include but are not limited to employees, students, parents, volunteers, contractors and occasional staff of the School.

Viruses and Malware: destructive computer programs that replicate or attach themselves to an existing program without authorization.

Website: a collection of related web pages containing digital content (text, images, videos, etc.) hosted on a web server accessible from the internet or a private network.

C. PROCEDURES

Administrative Procedures – All Users

These administrative procedures are established to:

- Increase safety for all community members
- Ensure alignment with the School's mission, vision and values
- Enhance teaching and learning
- Enhance relationships and community
- Improve efficiency of technology systems
- Enhance staff skills, knowledge and exchange of information with their peers.

All Users must abide by the administrative procedures outlined in this section.

1. Responsibilities

(a) The School recognizes that parents share responsibility for transmitting Catholic values to their children and providing guidance in the appropriate use of technology.

(b) The School provides Users with access to the School's sanctioned Electronic Communication system(s) based on their role in the School. These include but are not limited to: Microsoft Office 365 Suite, Edsby, School computers and School WIFI.

(c) The use of the School's Electronic Communication systems is a privilege, not a right, and as such can be restricted or, if appropriate, removed altogether.

(d) Users are expected to use the School's Electronic Communication systems in an ethical, lawful and appropriate manner as governed by applicable legislation, School policies and procedures.

(e) Through this Policy the School will notify Users about the School's Electronic Communication systems and the expectations governing its use.

(f) The School will expect educators to model and teach digital citizenship as appropriate to student age and ability.

(g) The School will provide opportunities for professional learning to School employees on the appropriate use of technological resources.

(h) The School will provide students and parents with guidelines for student safety and appropriate, ethical use of technology and the internet.

(i) For staff and existing Users, continued use of the School's Electronic Communication system, School Network and Technology will be interpreted by the School that the User has agreed to comply with the applicable School policies and procedures.

(j) The School Code of Conduct will be consistent with the regulations within this Policy.

(k) This Policy contains restrictions on accessing, storing and disseminating inappropriate material. There is a wide range of material available on the internet, some of which may not be consistent with governing laws nor with the values and code of ethics advocated by the School.

(l) The School will make every effort and has taken reasonable precautions to avoid the misuse of internet and Electronic Communication services. However, the possibility exists that Users may receive or access content that is not in line with this Policy. The School's internet content filtering system is considered a support to staff and not a replacement for properly supervising student access to the internet. Users who access inappropriate content despite the School's best efforts to prevent such an occurrence will be held responsible for their actions and appropriate disciplinary consequences will be applied.

(m) User acknowledgement forms will be provided prior to the start of each school year. These will be signed by all Users before they are granted access to the School's digital resources and Electronic Communication systems.

2. Personal Safety

(a) Users should protect their personal information and follow the available guidelines and resources published by the Information and Privacy Commissioner of Ontario (ipc.on.ca).

(b) Users shall protect their personal login credentials and not share these with anyone else.

3. Unacceptable Activities

(a) **Unauthorized Access** - Users will not attempt to gain unauthorized access to the School's system or to any other computer system through the School Network or go beyond their authorized access. This includes attempting to log on through another person's user account or accessing another person's files. Users will not access any other person's social media accounts, email, data or personal information without prior express written permission from that person.

(b) **Malicious Access** - Users will not make deliberate attempts to disrupt the performance of the computer system or destroy data by spreading computer viruses or by any other malicious means. These actions may be illegal and will be dealt with as such.

(c) **Illegal Activities** - Users will not use the School Network and Technology to engage in any illegal act, such as arranging for the sale or purchase of restricted substances such as alcohol and drugs, engaging in criminal activity, threatening the safety of a person, or engaging in uses that violate any federal or provincial laws, including the *Ontario Human Rights Code*, copyright, intellectual property or other laws, guidelines or agreements.

(d) **Cyberbullying / Threats / Harassment** - Users will not use the School Network and Technology to engage in inappropriate behaviours including, but not limited to, cyberbullying, personal attacks, threats, harassment, hate-motivated and discriminatory behaviours. Users who use the School Technology or use PEDs to engage in such inappropriate behaviours at School, School-related events or in a manner that negatively impacts the School climate may be subject to disciplinary measures including those outlined in the *Education Act*, the School Code of Conduct, and relevant legislation. Any action that is considered by the School Administration to be conduct injurious to the moral tone of the School will be dealt with according to the School Code of Conduct.

(e) **Inappropriate Language** - Users will maintain an appropriate professional tone in all communications.

(i) Inappropriate language includes but is not limited to:

- Use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, bullying, harassing, racist or disrespectful language;
- Posting information that, if acted upon, could cause damage to or disruption of resources and/or services; and
- Personal attacks, including prejudicial, discriminatory, libelous or slanderous attacks.

(ii) Restrictions against inappropriate language apply to public messages, private messages, and material posted on web sites.

(iii) Users will not knowingly or recklessly post false or defamatory information meant to harm the reputation of a person or an organization.

(f) **Inappropriate Content** - Users will not use the School Network and Technology to create, process, access, distribute, download, store, or share material that is illegal, profane, offensive, inappropriate, or obscene (e.g. pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (e.g. hate literature). Exceptions may be made if the purpose of such access is to conduct legitimate research, learning, and both the teacher and the parent of the student have provided prior approval for access.

If Users inadvertently access inappropriate content as defined above, they shall immediately disclose this incident to their teacher or immediate supervisor. This will protect Users against an allegation that they have intentionally violated this Policy.

(g) **Impersonation** - Users will not impersonate or employ a false identity in any Electronic Communication.

(h) **Unauthorized Equipment, Software and Media** – Users will not connect unauthorized equipment, install unauthorized software or distribute media files (where it violates the use terms of applicable software, licensing agreements, or copyright laws) on the School Network or Technology.

(i) **Commercial Use** - Users may not use the School Network and Technology for business or commercial purposes, defined as offering or providing goods or services which are unrelated to that person's duties and responsibilities at the School, or purchasing goods or services for personal use.

(j) **Political Lobbying** - Users may not use the School Network and Technology for political lobbying. However, School staff and students may use the system to analyze legislative measures and communicate with their elected representatives on political issues. Such views should not be disseminated to others.

4. Respect for Privacy

The use of information technology resources is monitored to help ensure the School Network and computing systems are available and that Users conform with this Policy in order to further health, safety and security for all Users and resources. **Users should have a limited expectation of privacy when using the School Network and Technology.**

(a) Users should be aware that the School monitors the operation of the School Network and Technology generally to alert IT staff of any service outages or anomalies. This information is collected in system logs. The information collected in the IT systems may be utilized or disclosed to trigger or augment an investigation for possible violation of law, School policy or procedures or employment obligations.

(b) The School has the right, but not the obligation, to inspect and monitor the use of the School Network or Technology, including, without limitation, inspecting the contents of voicemail, social media and Electronic Communication. Users will not necessarily be notified when such monitoring is to take place, or whether monitoring has occurred. In certain situations, the School may be compelled to access, read, copy, reproduce, print, retain, move, store, destroy and/or disclose messages, files or documents stored in or sent over the School Network or using School Technology. These situations may include, but are not limited to the following:

- in the course of regular maintenance of School Network or Technology;
- in the event of a request for documents as part of litigation or similar proceedings; or
- where the School has reason to believe that the School Network or Technology are being used in violation of this Policy.

(c) Users who require a private means of accessing or communicating data should use PEDs that are not connected to the School Network, in compliance with the School's policies governing the use of PEDs on School premises.

(d) Users will not alter the content of a message, without the permission of the original author who sent the message.

(e) Proper judgement should be exercised in deciding which messages are appropriate to forward to other recipients.

(f) Users will not distribute or forward chain letters, jokes, and inappropriate materials or engage in spam e-mails.

(g) Users shall respect an individual's personal privacy and will not share an individual's personal information without the direct permission of that individual.

5. Plagiarism and Copyright Infringement

(a) Plagiarism is taking the ideas, writings, or images of others and presenting them as if they were original to the User. Users will not plagiarize works that they find on the internet or elsewhere.

(b) Copyright is the protection of creative works and authors' rights. Users will respect the rights of copyright owners, including software manufacturers and providers of digital media. If the Users are unsure whether they can use a work, they should request permission from the copyright owner. For further information concerning this, consult the School's Access Copyright regulations.

(c) Content published on web sites must be original or written permission obtained for the use of such copyright material and its ownership fully acknowledged.

(d) Visitors and Users to the School public website may copy any information for their own personal use but may not otherwise publish or reproduce any such information in any manner, without the prior written consent of the School.

6. Web Sites

(a) All website content created by website publishers within the School framework must be consistent with the mission, values and educational aims of the School and must comply with all applicable legislation, School guidelines, policies and procedures.

(b) All website content created by website publishers within the School framework must adhere to defined web-page standards, formats and templates consistent with the branding of the School.

7. Bring Your Own Device / Personal Electronic Devices

(a) Any use of PEDs must comply with this Policy, and with all other applicable guidelines or policies of the School.

(b) The School assumes no responsibility for the theft, loss, recovery, repair or replacement of any PED brought onto School premises, whether the item is lost, stolen or taken by School Administration.

(c) During school hours, all PEDs shall be used for educational or professional purposes only. Students will only be permitted to use PEDs in a classroom with the expressed permission of the teacher.

(d) Users will keep smart and cellular phones on silent mode while on School premises.

(e) Users will connect their own PEDs to the School Network using their own Single Sign On (SSO) credentials as issued by the School.

(f) Students are not permitted to use personal hot spots or Virtual Private Networks (VPNs) to circumvent the School Network security.

(g) The IT department will not provide any support or troubleshooting of hardware, software or network connectivity issues on PEDs other than an approved device under the BYOD Policy. Support will only be available for issues pertaining to educational or professional usage.

(h) Unless legally licensed, Users will not install software licensed by the School on PEDs.

(i) Software licensed for home use by teachers and students by the School is only permitted within the provisions of the licensing agreement granted.

(j) Users will ensure that PEDs are protected (if applicable) with anti-virus malware protection software.

(k) If a PED is suspected to be interfering with the School Network and systems, the User will be required to cease connecting and using the PED on the School's premises.

(l) Any PED with image, video capture and recording capabilities are absolutely prohibited in areas where there is an expectation of privacy (e.g., washrooms, change rooms). The recording and taking of photographic images of a person or persons, on School property, at School events, and during School activities and/or hours, is prohibited without the permission of the person or persons being photographed or the principal or designate.

(m) The electronic transmission or posting of recordings and photographic images of a person or persons on School property, at School events, and during School activities

and/or hours, is prohibited without the permission of the person or persons being photographed or the principal or designate.

(n) The use of PEDs and images or recordings of activities that may negatively impact the School climate must not be captured, transmitted or posted under any circumstances.

(o) In the event of an emergency, lockdown, or evacuation of the School or building, an administrator will provide instruction to the community pertaining to the acceptable use of PEDs in the particular emergency conditions.

(p) All Users should be aware that in some instances transmission, recordings or images may be reviewed and relied on, even if obtained in a manner not wholly consistent with this Policy.

8. Limited Personal Use

(a) The limited personal use of computer technology, whether School provided or PEDs used on School premises, is permitted and is governed by these procedures.

(b) The limited personal use of computer technology must not interfere with School business, student learning, and with the User's duties and/or obligations.

(c) Subject to the above, Users shall engage in respectful and responsible Electronic Communication that is in line with these procedures and in the best interests of the School.

(d) This privilege of limited personal use may be revoked or limited at any time when utilizing School Technology.

9. Respect for Resource Limits

(a) Personal files and content not related to curriculum and School responsibilities and duties should not be stored on School computers, servers, and information systems.

(b) Users will avoid downloading large amounts of material. Time and storage space are limited resources. If it becomes necessary to download a large file, Users will do so at a time when the system is not being heavily used and immediately remove the file when no longer required. A reminder that the storage of copyrighted material for which consent has not be given is not permitted on School Technology or the School Network.

(c) Users will not engage in wasteful or forbidden use of the School Network or Technology.

10. System Security

(a) Users are responsible for the use of their individual account and should take reasonable precautions to prevent others from being able to use their account. Under no conditions should a User provide their user account and password to another person.

(b) Users will immediately notify a teacher or School administrator or IT administrator if they have identified a possible School Network or Technology security problem. Users are not authorized to deal with School Network or Technology security problems as this may be construed as an illegal attempt to gain access.

(c) Users will not attempt to disable or compromise the security of information contained on the School Network and Technology, and applicable external networks.

(d) Users will not vandalise or make deliberate attempts to damage the School Network or Technology. Vandalism also includes attempts to access or otherwise violate the integrity of private accounts, files or programs, the deliberate infecting of the network with a computer "virus," and attempts at "hacking" into any of the computers using any method.

(e) Users shall take reasonable precautions to protect the integrity of the School Network and Technology to prevent unauthorized access by others. For example, staff and students, before leaving computers or mobile devices unattended, shall do one or more of the following as applicable: i) use a password protected screen to lock the device or technology being used; ii) lock the room the device or technology is present in; and iii) not leave School Technology unsecured or unattended unless necessary.

11. Disciplinary Consequences

(a) Users' violation of this Policy will be handled in a fair manner subject to any obligations contained within applicable Collective Agreements, School Code of Conduct, legislations (i.e., *Teaching Profession Act*, Ontario College of Teachers Act, *Education Act*, etc.) or School policy and procedures.

(b) Disciplinary action will be tailored to meet specific concerns related to the violation and assist the User to conform to this Policy and model appropriate behaviour on an electronic network and computing system. The disciplinary action may include but is not limited to denying, restricting, or suspending User access to the School Network or Technology resources.

(c) Some violations may be an offence under Canada's Criminal Code. Appropriate legal authorities will be contacted if there is any suspicion of illegal activities. In accordance with the Police-School Protocol, the School will cooperate fully with legal authorities in any investigation relating to illegal activities conducted through the School Network or Technology, which may include providing authorities with information gathered through collection, inspection, monitoring or investigation.

12. Indemnification of the School

Users agree, by virtue of access to the School's Network, Technology, Electronic Communication system, computing systems, services or facilities, to indemnify, defend and hold harmless the School for any suits, claims, losses, expenses or damages, including but not limited to litigation costs and legal fees, arising from or related to the User's access to or use of the School's Network, Technology, Electronic Communication system, computing systems, services and facilities.

13. Release of Liability

The School makes no warranties of any kind, whether express or implied, with respect to the use of the School Network and Technology. The School will not be responsible for any damages Users suffer as a result of their use of the School Network and Technology. This includes loss of data resulting from delays, non-deliveries, delayed deliveries, service interruptions, the School's negligence, or the User's errors or omissions.

14. Third Party Terms of Service

By accessing certain third party services, Users are deemed to consent to the terms of service of the third party. The School does not have any control over third party terms of service.

Administrative Procedures - Students

In addition to the administrative procedures for All Users, the following section outlines additional administrative procedures applicable to all students enrolled in the School. All students must abide by the administrative procedures outlined in this section. In addition, students must refer to and abide by Appendix 1 – Social Media Policy – Students.

1. Personal Safety

Students will promptly disclose to a School administrator or educator any Electronic Communication that is inappropriate or makes them feel uncomfortable.

2. Bring Your Own Device / Personal Electronic Devices

(a) Students may use their own approved computer or tablet in the classroom for educational purposes and only when directed by the classroom teacher. At all other times, student use of a PED (e.g. smart phone, cell phone, smart watch, etc.) in the classroom is prohibited. A student who uses a PED in the classroom without teacher direction is subject to regular classroom and School disciplinary procedures.

(b) Students may use their own PED outside of the classroom only in designated areas and at designated times where PEDs are allowed according to School policy. Students

whose use of a PED contravenes School policy are subject to School disciplinary procedures.

(c) Students may only use PEDs (other than their approved laptop or tablet) before and after school and at lunch in the approved designated locations (as per mobile device policy).

(d) Students are not permitted to use PEDs in the hallways during the changeover between classes.

(e) PEDs are not allowed in examination rooms or during assessments unless prior approval has been granted by teacher or School Administration.

(f) When a PED is being used inappropriately by a student, the teacher will confiscate the PED and turn it over to an administrator who will securely store the PED until the matter is appropriately addressed.

(g) The School administrator will determine any other situations where the use of a PED is restricted or prohibited based on such use compromising School security, personal safety, individual privacy, academic integrity and negatively impacting on the School environment.

3. Disciplinary Consequences

In the event that a student has violated this Policy, the student (and parent/guardian when applicable) will be notified of the violation and will meet with the School administrator. The violation will be subject to the School's Progressive Discipline Policy.

Administrative Procedures - Staff

In addition to the administrative procedures for All Users, the following section outlines administrative procedures applicable to all School staff. All staff must abide by the administrative procedures outlined in this section. In addition, students must refer to and abide by Appendix 2 – Social Media Policy – Staff.

1. Personal Safety

(a) Any staff member that is in receipt of an inappropriate, harassing, obscene or offensive Electronic Communication that makes them feel uncomfortable or is a risk to their personal safety is to bring the matter to the attention of their immediate supervisor and appropriate Association and follow the protocol as outlined in the Policy on Workplace Harassment.

(b) Staff must not disclose personal contact information about students, other staff or other members of the School community. Personal contact information includes physical or electronic addresses, social media account information, identities, links or "handles",

pseudonyms, telephone numbers and other such personal information. Publication of pictures of individuals or a group requires the informed permission of all the individuals involved and, in the case of minors, of their parents or guardians.

(c) Staff must not publish photographs of students other than on the School websites, on School social media websites, pages or accounts, or in School publications even with express informed consent of all those involved, unless prior written consent and approval has been obtained from the relevant School authorities.

(d) Publication of information about School field trips (dates, times, locations) is forbidden to be communicated to people who are not directly entitled to such information or on public forums where unknown persons might access the information. This does not apply to publication of such information through private or access-controlled password-protected email, Intranet websites, or social media accounts or pages of the School.

2. Respect for Privacy

(a) Staff will have in their possession electronic copies of student data which is to be safeguarded per the Ontario Student Record Guidelines, Ontario Health Information Protection Act and Municipal Freedom of Information and Protection of Privacy Act. Any staff member who suspects data of this nature has been lost or access to such data compromised must notify their immediate supervisor and further report this incident to the School's Director of Human Resources. Each staff member will ensure that all communication is in compliance with applicable privacy legislation.

(b) Use of School E-mail Addresses and Distribution Lists - School e-mail addresses and distribution lists are not permitted for use by external individuals, organizations unless for School pre-approved business.

(c) Unauthorized access by any staff member of another staff member's electronic information is a violation of the School policy.

3. Personal Electronic Devices

(a) Users should not store any School confidential information (including but not limited to data and personal information of students, staff, etc.) on PEDs.

(b) Prohibited uses of PEDs by staff that may result in disciplinary action include, but are not limited to, the following:

- Use in any way that compromises the academic integrity of student assessment and evaluation;
- Use in any way that interferes with or disrupts the instructional day or the teaching/learning environment (i.e. using PEDs in classrooms, instructional spaces, hallways, stairwells, etc.);

- Use in any way that violates an individual's reasonable expectation of dignity and privacy (i.e. using PEDs in classrooms, teaching areas, change rooms, washrooms, hallways, stairwells or during a private meeting, etc.);
- Use in any way that compromises personal and/or School safety;
- Use in any way that facilitates the commission of a crime (i.e. using PEDs to break federal, provincial or municipal laws);
- Any other use of PEDs that compromises an individual's reputation or character or interferes with School security, personal safety, individual dignity and privacy or academic integrity;
- Use in any way to violate the copyright or other intellectual property rights of any other person, or to encourage anyone else to do so.

4. Limited Personal Use

The limited personal use of computer technology should only occur during staff members' non-work time (i.e. during breaks, lunches or outside of normal business hours) and not interfere with or affect a staff member's work performance.

5. System Security

When staff perform work at home, they shall not allow others, including family and household members, to use their School provided user account or device.

6. Intellectual Property

(a) Subject to any written agreement between the teacher and School, if a teacher voluntarily creates intellectual property ("**IP**") that is wholly outside of their teaching duties not utilizing any School resources whatsoever and is not utilized in any manner in the course of the teacher's employment, the intellectual property belongs to the teacher.

(b) If a staff member conceives, develops, creates or authors IP during the course of their employment with, or while performing their duties and responsibilities with the School, this IP is owned by the School. This includes IP created jointly with students while supervising coursework, extracurricular activities or special projects.

(c) Employers are encouraged to be cautious when sharing, posting, blogging or tweeting about IP they create, and to check with School authorities before doing so.

(d) If staff enter the School and its students in any contests, "hackathons" or competitions involving the IP, there may be additional rules that apply. Please consult with the School and read all contest rules before doing so.

(e) Staff must not use without prior express written authorization any material owned by the School, the School's confidential information, photographs, sounds or videos of students of the School, or any personal information pertaining to students or other staff members of the School, or members of the School community, including any information which may identify a student (such as information relating to education, timetable, curriculum, sports involvement, health, address, race, colour, ethnic origin, religion, age, sexual or gender orientation, family status, social media account information, user profiles, handles or portions of conversations, posts or messages sent or posted online or through mobile devices).

7. Software Use and Installation

(a) Prior to having any media, including open source software, placed on the School Network or Technology, Users shall obtain the prior approval of the School Administration and provide them with evidence of purchase of the software by the User, or evidence that the software is available legally and for free, a copy of the licence terms, and a description of the School purposes for which the media or software will be used.

(b) Users shall, at all times, respect the rights of copyright owners, including software manufacturers, and abide by the terms of all licence agreements relating to the School Technology and Network. A staff member who fails to comply with the terms of licence agreements or engages in other conduct that fails to respect the rights of copyright owners or violates this Policy may be subject to disciplinary action.

APPENDIX 1 – SOCIAL MEDIA POLICY – STUDENTS

INTRODUCTION

Social Media is defined as an internet-based community where members post information and media pertaining to themselves and have the opportunity to find and interact with other members, particularly those with shared real-life interests or experiences.

Social Media and Electronic Communication encompass software, applications, including those running on mobile devices, e-mail and websites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Facebook, Twitter, Flickr, YouTube, Wikipedia, Picasa, Snapchat.

Social Media is very popular with people of all ages and has become a virtual meeting place for students and School staff. Due to the wealth of new social media tools available to students, student products and documents have the potential to reach audiences far beyond the classroom. This translates into a greater level of responsibility and accountability for everyone.

GUIDELINES

Students of the School should adhere to the following guidelines when using social media and/or online tools:

- Be aware of what you post online. Social Media venues are very public. What you contribute leaves a digital footprint; therefore do not post anything that you would not want friends, parents, teachers or a future employer to see.
- Follow the School Code of Conduct when writing online. It is acceptable to disagree with someone else's opinion; however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.
- Be safe online. Never give out personal information, including but not limited to last names, telephone numbers, addresses, exact birthdates, credit card numbers and pictures. Do not share your password with anyone besides your teachers and parents.
- Linking to other websites to support your thoughts and ideas is recommended. Read the entire article prior to linking to ensure that all information is appropriate to a school setting.
- However, be careful what you link and repost to. Do not repost, reblog, retweet or reproduce content on your social media profile without first reading it. The School's policies regarding malicious, defamatory or infringing content may apply to your posts and what you hyperlink to as well. When using a hyperlink, be sure that the content is appropriate and adheres to the School's Responsible Use of Technology Policy.
- Do your own work. Do not plagiarize. Do not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste other's work. This includes blogs, videos, pictures, music performances, among other works.

When paraphrasing another's idea(s) be sure to cite your source with the URL. Follow the School's Code of Conduct and academic honesty policies. The School has a separate Copyright Policy for using copyrighted materials. Read and follow this, and other School policies carefully.

- How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
- Blog and wiki posts should be well-written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work, be sure it is in the spirit of improving the writing.
- If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell your teacher right away.
- You should not respond to any messages that make you feel uncomfortable or are threatening or intimidating.
- Consider reporting inappropriate conduct by anyone towards you to your teachers and parents/guardians.
- Think before posting content online. Online content is not deleted permanently. Do not post anything online you would not want your future employer to see.

Copyright

- Do not assume that content available online is in the public domain, or free for you to use. Respect copyright and other intellectual property laws and the works of others. The School has a separate Copyright Policy for using copyrighted materials (Access Copyright). Wherever possible, use materials that are available in the public domain and clearly marked as such (for instance, with the appropriate Creative Commons licenses: https://creativecommons.org/).
- Wherever possible, cite and link all your work. However, be careful that the content you are linking to is not malicious, discriminatory or against School policies or laws in any way.
- Software and resources downloaded must only be used under the terms and conditions specified by the creator or owner of the resource. If you are unsure, check with the School's IT Department. You must follow the School's Responsible Use of Technology Policy when using software on the School Network and Technology, or on School premises.
- Consider posting your own works online under a Creative Commons license, or clearly state online that you do not want anyone else to use your work without permission.

Profiles, Identity and Privacy

- Posting messages and attributing them to another user or otherwise misrepresenting one's identity online is unacceptable.

- Do not share passwords or accounts with others and make all efforts to protect this information from unauthorized users.
- Your personal information, including last name, address or phone numbers should not appear on blogs or wikis.
- When uploading digital pictures or avatars that represent yourself, make sure you select an appropriate image.
- Adhere to the School's Responsible Use of Technology Policy, Copyright Policy and other applicable policies.
- Do not share the School's or anyone else's confidential information online (such as their names, physical and online addresses, telephone or contact information, test results or grades).

Social Bookmarking

- Be aware that others can view the sites that you bookmark.
- Be aware of words to tag or describe the bookmark and of URL shortening services. Verify the landing to which they point before submitting a link as a bookmark. It would be best to utilize the original URL when naming a bookmark.
- Attempt to link directly to a page or resource, if possible, as you do not control what appears on landing pages in the future.
- Be careful when hyperlinking to another page. You must follow the School's Responsible Use of Technology Policy and Copyright Policy when doing so. Do not hyperlink to any content that would be considered unacceptable under these policies (such as copyright infringing material, or inappropriate websites/images/videos).

Privacy Settings and Content

- Set and maintain strict privacy settings by choosing settings that limit what others can do.
- Ensure that the privacy settings for content and photos are appropriately set and monitor who is able to post to any of your social media locations.
- Monitor regularly all content you or others post on your social media accounts and remove anything that is inappropriate.
- Ask others to remove any undesirable content related to you.
- Do not "troll" other people or organizations online. Respect the brand protection and copyright policies of every website/organization/brand you interact with.

Be a Responsible Digital Citizen

- Consider whether any posting may reflect poorly on you, your friends or the School.

- Do not post, publish or display any defamatory, abusive, obscene, threatening, intimidating, racially offensive, homophobic, sexist material.
- Alert School staff if you see other students being threatened, intimidated or bullied online.
- Be transparent and authentic. Do not "catfish" any person or organization for any reason, or encourage others to do so.
- Similarly, be cautious when interacting with others online. If an online interaction makes you uncomfortable or is inappropriate, do not hesitate to tell your teachers and parents/guardians immediately.
- Avoid impulsive, inappropriate or heated comments.
- Respect the privacy and confidentiality of personal information regarding other members of the School community.

Responsible Use Guidelines

- Use of the School Network and Technology is a privilege, not a right.
- Failure to comply with the School's Responsible Use of Technology Policy will result in loss of computer privileges and/or other consequences under the Code of Conduct.
- Any malicious attempt to harm or destroy data of any person, computer or network will result in appropriate disciplinary action.

APPENDIX 2 – SOCIAL MEDIA POLICY – STAFF

INTRODUCTION

Social Media is defined as an internet-based community where members post information and media pertaining to themselves and have the opportunity to find and interact with other members, particularly those with shared real-life interests or experiences.

Social Media and Electronic Communication encompass software, applications, including those running on mobile devices, e-mail and websites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Instagram, Facebook, Twitter, LinkedIn, Flickr, YouTube, Wikipedia, Picasa, Snapchat.

Professional Boundaries

Social Media is becoming increasingly popular with people of all ages and, in some cases, has become a virtual meeting place for School personnel and students. Maintaining professional boundaries in all forms of communication, technology-related or not, is vital to maintaining appropriate professional relationships with students, parents/guardians and other stakeholders.

The faculty of the School use social media to create professional interactive virtual communities for students and the School's wider community. Social Media enable connectivity in the School's community as parents/guardians, students and other stakeholders benefit from access to assignments and School updates or can engage with educational connections outside the classroom.

All staff must be aware that the educational use of social media and Electronic Communication requires cautious and professional use by everyone. School staff are governed by the School's Responsible Use of Technology Policy requiring respectful and responsible conduct.

Every staff member must know and maintain proper professional boundaries with students, even when students initiate electronic interaction. Staff members are prohibited from connecting to student's personal sites and can only engage in communication in the School's established curriculum and social media venues. It is up to staff members to know and respect proper professional boundaries with students, even when students initiate electronic interaction.

At all times School staff must use such social media tools in ways that are consistent with the mission and vision of the School and that comply with the Ontario College of Teachers' professional advisory entitled "Use of Electronic Communication and Social Media", approved on September 27, 2017.

The off-duty conduct of our staff members matters. Sound judgment and due care should be exercised by staff members at all times, even when off-duty. The Supreme Court of Canada has ruled that teacher's off-duty conduct, even when not strictly an exercise of one's job duties, is

relevant to their suitability to teach. School staff should maintain a sense of professionalism at all times – in their personal and professional lives. Avoiding improper, unethical or illegal activities is paramount in maintaining a safe and inclusive School environment.

GUIDELINES

School staff should adhere to the following guidelines when using online social media applications that may be frequented by current or former students of the School or their families:

Interact with Students Appropriately

- As a digital citizen, teachers will model the behaviour they expect to see online from their students.
- Alert students to appropriate online behaviour and the proper use of comments and images.
- School staff will maintain their professional persona by communicating with students electronically at appropriate times of the day and through established education platforms (i.e., a web page dedicated to a School program, project or class, or a School-approved communication platform such as Edsby).
- Maintain a formal, courteous and professional tone in all communications with students to ensure that professional boundaries with students are maintained.
- Avoid exchanging private texts, phone numbers, personal e-mail addresses or photos of a personal nature with students.
- Decline student-initiated "friend" requests and do not issue "friend" requests to students.
- Decline parent-initiated "friend" requests and do not issue "friend" requests to a parent.
- Social network "friend" requests may be accepted only with alumni over the age of 18.
- Notify parents/guardians and the applicable School administrators before using social media or networks for classroom activities. Please read the Responsible Use of Technology Policy and other School policies, as well as your employment policies carefully. Staff members may be required to request permission from the School to create social media accounts or pages or website for School-related activities.

Understand Privacy Concerns

School staff will:

- Set and maintain strict privacy settings by choosing settings that limit what others can do. Blanket invitations that use e-mail contacts automatically should be avoided. Students should not be among those who are allowed to post on a staff member's personal social media location but are welcome to publish through School sanctioned sites.
- Assume that information that they post can be accessed by the School.
- Monitor regularly all content that they or others post to their social media accounts and remove anything that is inappropriate.

- Ask others to remove any undesirable content related to them.
- Recognize that many former students have online connections with current students, and that information shared between such staff and former students is likely to be seen by current students as well.
- Monitor content on their own social media feeds, accounts and profiles, and remove inappropriate content from them.
- Maximise privacy and social media settings to ensure that students cannot view or post content to your profile.
- Join online communities and groups with discretion and by exercising caution.
- Recognize that anything posted online is traceable, even if deleted.
- Review the privacy settings and terms and conditions for digital media or communication platform or technology they use or join;
- Obtain the appropriate consent forms before posting student work, digital pictures or information about the School and School-related activities.
- Ensure that content they post does not infringe on copyright or other intellectual property laws of any person.
- Exercise caution when hyperlinking or reposting content, especially if the content is controversial or expresses views on individuals or organizations.

Act Professionally

- Respect the privacy and confidentiality of information pertaining to students, parents, staff and other members of the School community. Postings in personal blogs or websites shall not reveal confidential information about any member of the School community. This includes personal information, online pseudonyms or nicknames, photographs or videos of students or staff, financial information, School plans, marketing materials or School development information.
- School staff will consider whether any posting may reflect poorly on them, the School or the teaching profession. Social Media sites shall not be used to attack, threaten or intimidate colleagues. Staff members will respect the privacy and feelings of others.
- Be transparent and authentic. School staff must use their professional identity at all times. Staff who use social media for School purposes must do so using their own name or the name of the course, not a pseudonym or nickname.
- Do not post online criticism about students, colleagues, the School or others within the School community, including impulsive, inappropriate or heated comments.
- Ensure that comments do not incite others to make discriminatory, harassing or other professionally unacceptable comments. School staff will actively monitor their site, threads and blogs for inappropriate responses and, if necessary, follow up through established reporting protocols.

- School staff are aware of and will comply with the School's Responsible Use of Technology Policy and other policies regarding the use of social media/Electronic Communications and the appropriate use of electronic equipment.

School-operated Social Media Accounts

- Only authorized Staff members may use or post on School-operated and owned social media accounts and profiles.

- Linking to School social media accounts and profiles, such as through "@" replies, using hashtags or giving online "shout outs" should be done with discretion and in keeping with staff members' obligations under other School policies and rules.